STATE OF MONTANA

Montana Information Security Advisory Council

Best Practices Workgroup – Disposal of Media Storage Device Procedure

Disposal of Media Storage Device Procedure

1. Purpose

   This procedure identifies the steps used for disposing of media storage devices. It meets the requirements for the State Enterprise Information Security Policy.
   It is a requirement to protect IT assets by 1) destruction of the IT device or 2) complete removal of all electronic data from the media storage devices.

2. Policy
   Disposal of Media Storage Device Procedure applies to the following controls found within the Information Security Policy.
   a. Information Security Policy
      - Protect
        - 2.9.3.4
        - 2.13
        - 2.18.3
   b. Information Security Policy – Appendix A
      - Media Protection (MP)
        - MP-4 – Media Storage
        - MP-6 – Media Sanitization

3. Recommended Best-Practices to be Adopted as Standard Configuration

Media Storage Device is defined by any device that stores and records data. Examples may include; internal and external hard-drives in workstations, servers, printers, copiers, portable storage devices (USBs), laptops, tablets, CD's, DVD's, audio recorders, memory, etc.

All media storage devices must be sanitized prior to disposal. If sanitization cannot be completed, the media storage must be reset to factory state or destroyed. Media storage on leased equipment may be destroyed before equipment is returned.

Agency IT personnel should use a sanitation program that complies with NIST requirements and will effectively sanitize the media storage device. Employed sanitation mechanisms (strength and integrity) must meet the classification and sensitivity of the information.

Destruction process:

1. In the event a disk cannot be properly wiped because it is failing or not compatible with our wiping process, it is sent to Ewaste.
2. The Ewaste partner destroys all disks with their disk shredder.
3. All destruction must be completed on site.

Solid state drives must be sanitized using an authenticated tool. The wiping will be validated and tape will be placed over the drive to identify that the device has been wiped.

If a device cannot be sanitized, the system will be destroyed.

Documentation

Agency directors are responsible for maintaining documentation on all electronic data storage devices (e.g., PCs, laptops, servers, portable devices) that have been either destroyed or sanitized. These records must be retained by the agency for six years. The disposal records shall contain the following information:

1. Employee name performing cleaning
2. Date of cleaning
3. Device Type
4. Device(s) identification (vendor serial number or Dell service tag number)

5. Method of Sanitization
6. Destination of device
7. Disposing Agency

Summary of Sanitization Methods

Table 5-1: Sanitization Methods

Method	Description
Clear	One method to sanitize media is to use software or hardware products to overwrite useraddressable storage space on the media with non-sensitive data, using the standard read and write commands for the device. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also should include all useraddressable locations. The security goal of the overwriting process is to replace Target Data with non-sensitive data. Overwriting cannot be used for media that are damaged or not rewriteable, and may not address all areas of the device where sensitive data may be retained. The media type and size may also influence whether overwriting is a suitable sanitization method. For example, flash memory-based storage devices may contain spare cells and perform wear levelling, making it infeasible for a user to sanitize all previous data using this approach because the device may not support directly addressing all areas where sensitive data has been stored using the native read and write interface. The Clear operation may vary contextually for media other than dedicated storage devices, where the device (such as a basic cell phone or a piece of office equipment) only provides the ability to return the device to factory state (typically by simply deleting the file pointers) and does not directly support the ability to rewrite or apply media-specific techniques to the non-volatile storage contents. Where rewriting is not supported, manufacturer resets and procedures that do not include rewriting might be the only option to Clear the device and associated media. These still meet the definition for Clear as long as the device interface available to the user does not facilitate retrieval of the Cleared data.
Purge	Some methods of purging (which vary by media and must be applied with considerations described further throughout this document) include overwrite, block erase, and Cryptographic Erase, through the use of dedicated, standardized device sanitize commands that apply media-specific techniques to bypass the abstraction inherent in typical read and write commands. Destructive techniques also render the device Purged when effectively applied to the appropriate media type, including incineration, shredding, disintegrating, degaussing, and pulverizing. The common benefit across all these approaches is assurance that the data is infeasible to recover using state of the art laboratory techniques. However, Bending, Cutting, and the use of some emergency procedures (such as using a firearm to shoot a hole through a storage device) may only damage the media as portions of the media may remain undamaged and therefore accessible using advanced laboratory techniques. Degaussing renders a Legacy Magnetic Device Purged when the strength of the degausser is carefully matched to the media coercivity. Coercivity may be difficult to determine based only on information provided on the label. Therefore, refer to the device manufacturer for coercivity details. Degaussing should never be solely relied upon for flash memory-based storage devices or

	for magnetic storage devices that also contain non-volatile non-magnetic storage. Degaussing renders many types of devices unusable (and in those cases, Degaussing is also a Destruction technique).
Method	**Description**
Destroy	There are many different types, techniques, and procedures for media Destruction. While some techniques may render the Target Data infeasible to retrieve through the device interface and unable to be used for subsequent storage of data, the device is not considered Destroyed unless Target Data retrieval is infeasible using state of the art laboratory techniques. • *Disintegrate, Pulverize, Melt, and Incinerate*. These sanitization methods are designed to completely Destroy the media. They are typically carried out at an outsourced metal Destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. • *Shred*. Paper shredders can be used to Destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. To make reconstructing the data even more difficult, the shredded material can be mixed with non-sensitive material of the same type (e.g., shredded paper or shredded flexible media). The application of Destructive techniques may be the only option when the media fails and other Clear or Purge techniques cannot be effectively applied to the media, or when the verification of Clear or Purge methods fails (for known or unknown reasons).

Sanitization and Disposition Decision Flow

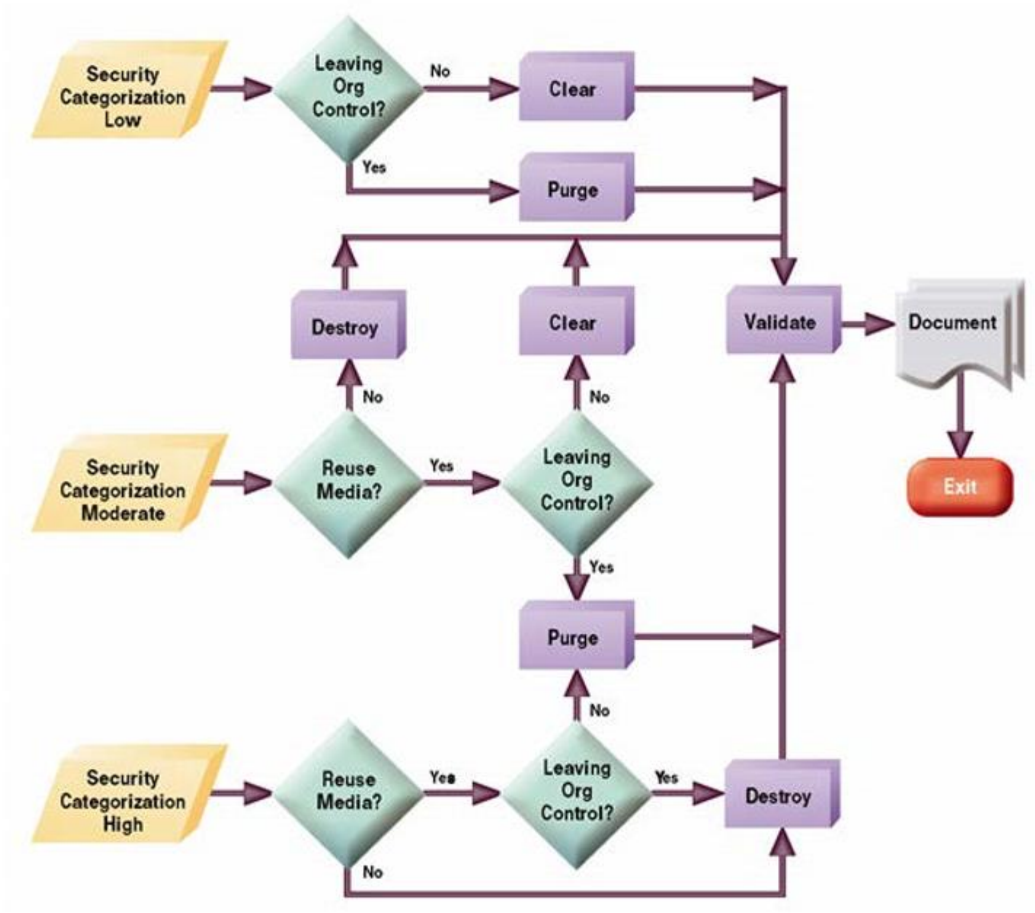

Figure 4-1: Sanitization and Disposition Decision Flow

Minimum Sanitization Recommendations

See Disposal of Computer or Electronic Storage Device Form – Appendix A

See Disposal of Media Storage Device Procedure – Appendix B for Minimum Sanitization Recommendations.

Recommendations are from NIST Special Publication 800-88 Revision 1 (December 2014) - Guidelines for Media Sanitization. **Please refer to NIST for most current version and recommendations.

4. Compliance

Compliance shall be evidenced by implementing Disposal of Media Storage Device as described above. Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this Disposal of Media Storage Device procedure are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form. Changes to policies and standards will be prioritized and acted upon based on impact and need.

Definitions:
Terms and definitions are identified in the National Institute of Standards and Technology (NIST) Glossary of Key Information Security Terms and Guidelines for Media Sanitization.

References:
NIST Special Publication 800-88 Revision 1 (December 2014) - Guidelines for Media Sanitization

Appendix A

MT-ISAC Best Practice

Disposal of Computer or Electronic Storage Device Form

Disposal Information

Individual responsible for cleaning: Click here to enter name	Date: Click here to enter a date.
Device Type: Choose an item.	Asset Number(s):
Method of Sanitization or Destruction: Choose an item.	
Destination of device: Choose an item.	If selected Other please explain: Click here
Sanitized by (type name):	
Disposing Agency:	
Comments: Click here	

Appendix B

Minimum Sanitization Recommendations

Recommendations are from NIST Special Publication 800-88 Revision 1 (December 2014) - Guidelines for Media Sanitization. **Please refer to NIST for most current version and recommendations.

Table A-1: Hard Copy Storage Sanitization

Hard Copy Storage	
Paper and microforms	
Clear:	N/A, see Destroy.
Purge:	N/A, see Destroy
Destroy:	Destroy paper using cross cut shredders which produce particles that are 1 mm x 5 mm (0.04 in. x 0.2 in.) in size (or smaller), or pulverize/disintegrate paper materials using disintegrator devices equipped with a 3/32 in. (2.4 mm) security screen. Destroy microforms (microfilm, microfiche, or other reduced image photo negatives) by burning.
Notes:	When material is burned, residue must be reduced to white ash.

Table A-2: Networking Device Sanitization

Networking Devices	
Routers and Switches (home, home office, enterprise)	
Clear:	Perform a full manufacturer's reset to reset the router or switch back to its factory default settings.
Purge:	See Destroy. Most routers and switches only offer capabilities to Clear (and not Purge) the data contents. A router or switch may offer Purge capabilities, but these capabilities are specific to the hardware and firmware of the device and should be applied with caution. Refer to the device manufacturer to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.

Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	For both Clear and (if applicable) Purge, refer to the manufacturer for additional information on the proper Sanitization procedure. Network Devices may contain removable storage. The removable media must be removed and sanitized using media-specific techniques.

Table A-3: Mobile Device Sanitization

Mobile Devices **(If a device has removable storage – first check for encryption and unencrypt if so – then remove the removable storage prior to sanitization)**	
Apple iPhone and iPad (current generation and future iPhones and iPads)	
Clear:	Select the full sanitize option (typically in the 'Settings > General > Reset > Erase All Content and Settings' menu). (The sanitization operation should take only minutes as Cryptographic Erase is supported. This assumes that encryption is on and that all data has been encrypted.) Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results.
Purge:	Select the full sanitize option (typically in the 'Settings > General > Reset > Erase All Content and Settings' menu). (The sanitization operation should take only minutes with Cryptographic Erase being supported. This assumes that encryption is on and that all data has been encrypted.)
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Following the Clear/Purge operation, manually navigate to multiple areas of the device (such as browser history, files, photos, etc.) to verify that no personal information has been retained on the device. Before sanitizing the device, ensure that the data is backed up to a safe place. Current iPhones have hardware encryption – turned on by default.
Blackberry	**(back up data on device before sanitization)**
Clear:	BB OS 7.x/6.x - Select Options > Security Options > Security Wipe , making sure to select all subcategories of data types for sanitization. Then type "blackberry" in the text field, then click on "Wipe" ("Wipe Data" in BB OS 6.x) BB OS 10.x (Decrypt media card before continuing) Select Settings, Security and Privacy, Security Wipe . Type "blackberry" in the text field, then click on "Delete Data". The sanitization operation may take as long as several hours depending on the media size. Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results.

Purge:	BB OS 7.x/6.x - Select Options > Security > Security Wipe, then make sure to select all subcategories of data types for sanitization. Then type "blackberry" in the text field, then click on "Wipe" ("Wipe Data" in BB OS 6.x). For BB OS 10.x Select Settings> Security and Privacy>Security Wipe. Type "blackberry" in the text field, then click on "Delete Data". The sanitization operation may take as long as several hours depending on the media size.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Following the Clear/Purge operation, manually navigate to multiple areas of the device (such as browser history, files, photos, etc.) to verify that no personal information has been retained on the device. Centralized management (BES) allows for device encryption. Refer to the manufacturer for additional information on the proper sanitization procedure, and for details about implementation differences between device versions and OS versions. Proper initial configuration using guides such as the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) (http://iase.disa.mil/stigs/) helps ensure that the level of data protection and sanitization assurance is as robust as possible. If the device contains removable storage media, ensure that the media is sanitized using appropriate mediadependent procedures.
Devices running the Google Android OS	**(connect to power before starting encryption)**
Clear:	Perform a factory reset through the device's settings menu. For example, on Samsung Galaxy S5 running Android 4.4.2, select settings, then, under User and Backup, select Backup and reset, then select Factory data reset. For other versions of Android and other mobile phone devices, refer to the user manual. Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results.
Purge:	The capabilities of Android devices are determined by device manufacturers and service providers. As such, the level of assurance provided by the factory data reset option may depend on architectural and implementation details of a particular device. Devices seeking to use a factory data reset to purge media should use the eMMC Secure Erase or Secure Trim command, or some other equivalent method (which may depend on the device's storage media). Some versions of Android support encryption, and may support Cryptographic Erase. Refer to the device manufacturer (or service provider, if applicable) to identify whether the device has a Purge capability that applies media-dependent sanitization techniques or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.

Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Proper initial configuration using guides such as the DISA STIGs (http://iase.disa.mil/stigs/) helps ensure that the level of data protection and sanitization assurance is as robust as possible. Following the Clear or (if applicable) Purge operation, manually navigate to multiple areas of the device (such as browser history, files, photos, etc.) to verify that no personal information has been retained on the device. When in doubt, check device manual or call tech support. For both Clear and Purge, refer to the manufacturer for additional information on the proper sanitization procedure.
Windows Phone OS 7.1/8/8.x	**(Centralized management may be needed for encryption)**
Clear:	Select the Settings option (little gear symbol) from the live tile or from the app list. On the “Settings” page, scroll to the bottom of the page and select the “About” button. In the about page, there will be a **reset your phone** button at the bottom of the page. Click on this button to continue. Choose Yes when you see the warning messages. Please note that after the process is completed, all your personal content will disappear. Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results.
Purge:	The capabilities of Windows Phone devices are determined by device manufacturers and service providers. As such, the level of assurance provided by the factory data reset
	option may depend on architectural and implementation details of a particular device. Devices seeking to use a factory data reset to purge media should use the eMMC Secure Erase or Secure Trim command, or some other equivalent method (which may depend on the device’s storage media). In some environments, Windows Phone devices may support encryption, and may support Cryptographic Erase. Refer to the device manufacturer (or service provider, if applicable) to identify whether the device has a Purge capability that applies media-dependent sanitization techniques or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Following the Clear/Purge operation, manually navigate to multiple areas of the device (such as browser history, files, photos, etc.) to verify that no personal information has been retained on the device. Before sanitizing your device, ensure that you back up your data to a safe location. Refer to the manufacturer for proper sanitization procedure, and for details about implementation differences between device versions and OS versions. Proper initial configuration using guides such as the DISA STIGs (http://iase.disa.mil/stigs/) helps ensure that the level of data protection and sanitization assurance is as robust as possible.

All other mobile devices *This includes cell phones, smart phones, PDAs, tablets, and other devices not covered in the preceding mobile categories.*	
Clear:	Manually delete all information, then perform a full manufacturer's reset to reset the mobile device to factory state. Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results.
Purge:	See Destroy. Many mobile devices only offer capabilities to Clear (and not Purge) the data contents. A mobile device may offer Purge capabilities, but these capabilities are specific to the hardware and software of the device and should be applied with caution. The device manufacturer should be referred to in order to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Following the Clear or (if applicable) Purge operation, manually navigate to multiple areas of the device (such as call history, browser history, files, photos, etc.) to verify that no personal information has been retained on the device. For both Clear and (if applicable) Purge, refer to the manufacturer for proper sanitization procedure.

Table A-4: Equipment Sanitization

Equipment	
Office Equipment *This includes copy, print, fax, and multifunction machines*	
Clear:	Perform a full manufacturer's reset to reset the office equipment to its factory default settings.
Purge:	See Destroy. Most office equipment only offers capabilities to Clear (and not Purge) the data contents. Office equipment may offer Purge capabilities, but these capabilities are specific to the hardware and firmware of the device and should be applied with caution. Refer to the device manufacturer to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers. Office equipment may have removable storage media, and if so, media-dependent sanitization techniques may be applied to the associated storage device.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.

Notes:	For both Clear and (if applicable) Purge, manually navigate to multiple areas of the device (such as stored fax numbers, network configuration information, etc.) to verify that no personal information has been retained on the device. For both Clearing and (if applicable) Purge, the ink, toner, and associated supplies (drum, fuser, etc.) should be removed and destroyed or disposed of in accordance with applicable law, environmental, and health considerations. Some of these supplies may retain impressions of data printed by the machine and therefore could pose a risk of data exposure, and should be handled accordingly. If the device is functional, one way to reduce the associated risk is to print a blank page, then an all-black page, then another blank page. For devices with dedicated color components (such as cyan, magenta, and yellow toners and related supplies), one page of each color should also be printed between blank pages. The resulting sheets should be handled at the confidentiality of the Office Equipment (prior to sanitization). Note that these procedures do not apply to supplies such as ink/toner on a one-time use roll, as they are typically not used again and therefore will not be addressed by sending additional pages through the equipment. They will, however, still need to be removed and destroyed. Office Equipment supplies may also pose health risks, and should be handled using appropriate procedures to minimize exposure to the print components and toner. For both Clear and (if applicable) Purge, refer to the manufacturer for additional information on the proper sanitization procedure.

Table A-5: Magnetic Media Sanitization

Magnetic Media	
Floppies	
Clear:	Overwrite media by using organizationally approved software and perform verification on the overwritten data. The Clear pattern should be at least a single write pass with a fixed data value, such as all zeros. Multiple write passes or more complex values may optionally be used.
Purge:	Degauss in an organizationally approved degausser rated at a minimum for the media.
Destroy:	Incinerate floppy disks and diskettes by burning in a licensed incinerator or Shred.
Magnetic Disks (flexible or fixed)	
Clear:	Overwrite media by using organizationally approved software and perform verification on the overwritten data. The Clear pattern should be at least a single write pass with a fixed data value, such as all zeros. Multiple write passes or more complex values may optionally be used.

Purge:	Degauss in an organizationally approved degausser rated at a minimum for the media.
Destroy:	Incinerate disks and diskettes by burning in a licensed incinerator or Shred.
Notes:	Degaussing magnetic disks typically renders the disk permanently unusable.
Reel and Cassette Format Magnetic Tapes	
Clear:	Re-record (overwrite) all data on the tape using an organizationally approved pattern, using a system with similar characteristics to the one that originally recorded the data. For example, overwrite previously recorded sensitive VHS format video signals on a comparable VHS format recorder. All portions of the magnetic tape should be overwritten one time with known nonsensitive signals. Clearing a magnetic tape by re-recording (overwriting) may be impractical for most applications since the process occupies the tape transport for excessive time periods.
Purge:	Degauss the magnetic tape in an organizationally approved degausser rated at a minimum for the media.
Destroy:	Incinerate by burning the tapes in a licensed incinerator or Shred.
Notes:	Preparatory steps for Destruction, such as removing the tape from the reel or cassette prior to Destruction, are unnecessary. However, segregation of components (tape and reels or cassettes) may be necessary to comply with the requirements of a Destruction facility or for recycling measures.
ATA Hard Disk Drives *This includes PATA, SATA, eSATA, etc*	
Clear:	Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools. The Clear pattern should be at least a single write pass with a fixed data value, such as all zeros. Multiple write passes or more complex values may optionally be used.

Purge:	Four options are available: 1. Use one of the ATA Sanitize Device feature set commands, if supported, to perform a Sanitize operation. One or both of the following options may be available: a. The overwrite EXT command. Apply one write pass of a fixed pattern across the media surface. Some examples of fixed patterns include all zeros or a pseudorandom pattern. A single write pass should suffice to Purge the media. *Optionally:* Instead of one write pass, use three total write passes of a pseudorandom pattern, leveraging the invert option so that the second write pass is the inverted version of the pattern specified. b. If the device supports encryption and the technical specifications described in this document have been satisfied, the Cryptographic Erase (also known as CRYPTO SCRAMBLE EXT) command. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite command is not supported, the Secure Erase or the Clear procedure could alternatively be applied following Cryptographic Erase. 2. Use the ATA Security feature set's SECURE ERASE UNIT command, if support, in Enhanced Erase mode. The ATA Sanitize Device feature set commands are preferred over the over the ATA Security feature set SECURITY ERASE UNIT command when supported by the ATA device. 3. Cryptographic Erase through the Trusted Computing Group (TCG) Opal Security Subsystem Class (SSC) or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed (if the requirements described in this document have been satisfied). Refer to the TCG and device manufacturers for more information. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite command is not supported, the Secure Erase or the Clear procedure could alternatively be applied following Cryptographic Erase. 4. Degauss in an organizationally approved automatic degausser or disassemble the hard disk drive and Purge the enclosed platters with an organizationally approved degaussing wand.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.

Notes:	Verification must be performed for each technique within Clear and Purge, except degaussing. The assurance provided by degaussing depends on selecting an effective degausser, applying it appropriately and periodically spot checking the results to ensure it is working as expected. When using the three pass ATA sanitize overwrite procedure with the invert option, the verification process would simply search for the original pattern (which would have been written again during the third pass). The storage device may support configuration capabilities that artificially restrict the ability to access portions of the media as defined in the ATA standard, such as a Host Protected Area (HPA), Device Configuration Overlay (DCO), or Accessible Max Address. Even when a dedicated sanitization command addresses these areas, their presence may affect the ability to reliably verify the effectiveness of the sanitization procedure if left in place. Any configuration options limiting the ability to access the entire addressable area of the storage media should be reset prior to applying the sanitization technique. Recovery data, such as an OEM-provided restoration image may have been stored in this manner, and sanitization may therefore impact the ability to recover the system unless reinstallation media is also available. When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully. A quick sampling verification as described in section 4.7 should also be performed after any additional techniques are applied following Cryptographic Erase. Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified in this guidance and in Appendix D. Given the variability in implementation of the ATA Security feature set SECURITY ERASE UNIT command, use of this command is not recommended without first consulting with the manufacturer to verify that the storage device's model-specific implementation meets the needs of the organization. This guidance applies to Legacy Magnetic media only, and it is critical to verify the media type prior to sanitization. Note that emerging media types, such as HAMR media or hybrid drives may not be easily identifiable by the label. Refer to the manufacturer for details about the media type in a storage device. Degaussing the media in a storage device typically renders the device unusable.
SCSI Hard Disk Drives *This includes Parallel SCSI,Serial Attached SCSI (SAS), Fibre Channel, USB Attached Storage (UAS), and SCSI Express Partial sanitization is not supported in this section.*	
Clear:	Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools. The Clear procedure should consist of at least one pass of writes with a fixed data value, such as all zeros. Multiple passes or more complex values may optionally be used.
Purge:	Four options are available:

	1. Apply the SCSI SANITIZE command, if supported. One or both of the following options may be available: a. The OVERWRITE service action. Apply one write pass of a fixed pattern across the media surface. Some examples of fixed patterns include all zeros or a pseudorandom pattern. A single write pass should suffice to Purge the media. *Optionally:* Instead of one write pass, use three total write passes of a pseudorandom pattern, leveraging the invert option so that the second write pass is the inverted version of the pattern specified. b. If the device supports encryption, the CRYPTOGRAPHIC ERASE service action. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite command is not supported, the Clear procedure could alternatively be applied. 2. Cryptographic Erase through the TCG Opal SSC or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed. Refer to the TCG and vendors shipping TCG Opal or Enterprise storage devices for more information. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite command is not supported, the Clear procedure could alternatively be applied. 3. Degauss in an organizationally approved automatic degausser or disassemble the hard disk drive and Purge the enclosed platters with an organizationally approved degaussing wand. The degausser/wand should be rated sufficient for the media.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.

Notes:	Verification must be performed for each technique within Clear and Purge as described in the Verify Methods subsection, except degaussing. The assurance provided by degaussing depends on selecting an effective degausser, applying it appropriately and periodically spot checking the results to ensure it is working as expected. When using the three pass SCSI sanitize overwrite procedure with the invert (also known as complement) option, the verification process would simply search for the original pattern (which would have been written again during the third pass). While it is widely accepted that one pass of overwriting should be sufficient for Purging the data, the availability of a dedicated command that incorporates the ability to invert the data pattern allows an efficient and effective approach that mitigates any residual risk associated with variations in implementations of magnetic recording features across device manufacturers. The storage device may support configuration capabilities that artificially restrict the ability to access portions of the media, such as "SCSI mode parameter block descriptor's NUMBER OF LOGICAL BLOCKS field (accessible with the SCSI MODE SENSE and MODE SELECT commands". Even when a dedicated sanitization command addresses these areas, their presence may affect the ability to reliably verify the effectiveness of the sanitization procedure if left in place. Any configuration options limiting the ability to access the entire addressable area of the storage media should be reset prior to applying the sanitization technique. When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully. A quick sampling verification as described in the Verify Methods subsection should also be performed after any additional techniques are applied following Cryptographic Erase. Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified in this guidance and in Appendix D. This guidance applies to Legacy Magnetic media only, and it is critical to verify the media type prior to sanitization. Note that emerging media types, such as HAMR media or hybrid drives may not be easily identifiable by the label. Refer to the manufacturer for details about the media type in a storage device.
	Degaussing the media in a storage device typically renders the device unusable.

Table A-6: Peripherally Attached Storage Sanitization

Peripherally Attached Storage	
External Locally Attached Hard Drives *This includes, USB, Firewire, etc. (Treat eSATA as ATA Hard drive.)*	
Clear:	Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear pattern should be at least a single pass with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used.

Purge:	The implementation of External Locally Attached Hard Drives varies sufficiently across models and vendors that the issuance of any specific command to the device may not reasonably and consistently assure the desired sanitization result. When the external drive bay contains an ATA or SCSI hard drive, if the commands can be delivered natively to the device, the device may be sanitized based on the associated mediaspecific guidance. However, the drive could be configured in a vendor-specific manner that precludes sanitization when removed from the enclosure. Additionally, if sanitization techniques are applied, the hard drive may not work as expected when reinstalled in the enclosure. Refer to the device manufacturer to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting, block erasing, Cryptographic Erase, etc.) to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Verification as described in the Verify Methods subsection must be performed for each technique within Clear and Purge. Some external locally attached hard drives, especially those featuring security or encryption features, may also have hidden storage areas that might not be addressed even when the drive is removed from the enclosure. The device vendor may leverage proprietary commands to interact with the security subsystem. Please refer to the manufacturer to identify whether any reserved areas exist on the media and whether any tools are available to remove or sanitize them, if present.

Table A-7: Optical Media Sanitization

Optical Media	
CD, DVD, BD	
Clear/ Purge:	N/A
Destroy:	Destroy in order of recommendations: 1. Removing the information-bearing layers of CD media using a commercial optical disk grinding device. Note that this applies only to CD and not to DVD or BD media 2. Incinerate optical disk media (reduce to ash) using a licensed facility. 3. Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimensions of 0.5 mm and surface area of 0.25 mm² or smaller.

Table A-8: Flash Memory-Based Storage Device Sanitization

Flash Memory-Based Storage Devices	

ATA Solid State Drives (SSDs) *This includes PATA, SATA, eSATA, etc.*	
Clear:	1. Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear procedure should consist of at least one pass of writes with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used. Note: It is important to note that overwrite on flash-based media may significantly reduce the effective lifetime of the media and it may not sanitize the data in unmapped physical media (i.e., the old data may still remain on the media). 2. Use the ATA Security feature set's SECURITY ERASE UNIT command, if supported.
Purge:	Three options are available: 1. Apply the ATA sanitize command, if supported. One or both of the following options may be available: a. The block erase command. *Optionally:* After the block erase command is successfully applied to a device, write binary 1s across the user addressable area of the storage media and then perform a second block erase. b. If the device supports encryption, the Cryptographic Erase (also known as sanitize crypto scramble) command. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erase command is not supported, Secure Erase or the Clear procedure could alternatively be applied. 2. Cryptographic Erase through the TCG Opal SSC or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed. Refer to the TCG and vendors shipping TCG Opal or Enterprise storage devices for more information. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erase command is not supported, Secure Erase or the Clear procedure could alternatively be applied.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Verification must be performed for each technique within Clear and Purge as described in the Verify Methods subsection. When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully. A quick sampling verification as described in the Verify Methods subsection should also be performed after any additional techniques are applied following Cryptographic Erase.

	The storage device may support configuration capabilities that artificially restrict the ability to access portions of the media as defined in the ATA standard, such as a Host Protected Area (HPA), Device Configuration Overlay (DCO), or Accessible Max Address. Even when a dedicated sanitization command addresses these areas, their presence may affect the ability to reliably verify the effectiveness of the sanitization procedure if left in place. Any configuration options limiting the ability to access the entire addressable area of the storage media should be reset prior to applying the sanitization technique. Recovery data, such as an OEM-provided restoration image may have been stored in this manner, and sanitization may therefore impact the ability to recover the system unless reinstallation media is also available. Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified in this guidance and in Appendix D. Given the variability in implementation of the Enhanced Secure Erase feature, use of this command is not recommended without first referring the manufacturer to identify that the storage device's model-specific implementation meets the needs of the organization. Whereas ATA Secure Erase was a Purge mechanism for magnetic media, it is only a Clear mechanism for flash memory due to variability in implementation and the possibility that sensitive data may remain in areas such as spare cells that have been rotated out of use. Degaussing must not be solely relied upon as a sanitization technique on flash memory-based storage devices or on hybrid devices that contain non-volatile flash memory storage media. Degaussing may be used when non-volatile flash memory media is present if the flash memory components are sanitized using media-dependent techniques.
SCSI Solid State Drives (SSSDs) *This includes Parallel SCSI, Serial Attached SCSI (SAS), Fibre Channel, USB Attached Storage (UAS), and SCSI Express.*	
Clear:	Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear procedure should consist of at least one pass of writes with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used. Note: It is important to note that overwrite on flash-based media may significantly reduce the effective lifetime of the media and it may not sanitize the data in unmapped physical media (i.e., the old data may still remain on the media).

Purge:	Two options are available: 1. Apply the SCSI SANITIZE command, if supported. One or both of the following options may be available: a. The BLOCK ERASE service action. b. If the device supports encryption, the CRYPTOGRAPHIC ERASE service action. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erase command is not supported, the Clear procedure could alternatively be applied. 2. Cryptographic Erase through the TCG Opal SSC or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed. Refer to the TCG and vendors shipping TCG Opal or Enterprise storage devices for more information. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erase command is not supported, the Clear procedure is an acceptable alternative.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Verification must be performed for each technique within Clear and Purge as described in the Verify Methods subsection. The storage device may support configuration capabilities that artificially restrict the ability to access portions of the media, such as SCSI mode select. Even when a dedicated sanitization command addresses these areas, their presence may affect the ability to reliably verify the effectiveness of the sanitization procedure if left in place. Any configuration options limiting the ability to access the entire addressable area of the storage media should be reset prior to applying the sanitization technique. When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully. A quick sampling verification as described in the Verify Methods subsection should also be performed after any additional techniques are applied following Cryptographic Erase. Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified in this guidance and in Appendix D. Degaussing must not be performed as a sanitization technique on flash memory-based storage devices.
NVM Express SSDs	
Clear:	Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear procedure should consist of at least one pass of writes with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used.

Purge:	Two options are available: 1. Apply the NVM Express Format command, if supported. One or both of the following options may be available: a. The User Data Erase command. b. If the device supports encryption, the Cryptographic Erase command. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the User Data Erase command (if supported) to erase the media. If the User Data Erase command is not supported, the Clear procedure could alternatively be applied. 2. Cryptographic Erase through the TCG Opal SSC or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed. Refer to the TCG and vendors shipping TCG Opal or Enterprise storage devices for more information. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the User Data Erase command (if supported) to erase the media. If the User Data Erase command is not supported, the Clear procedure is an acceptable alternative.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Verification must be performed for each technique within Clear and Purge. When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully. A quick sampling verification as described in the Verify Methods subsection should also be performed after any additional techniques are applied following Cryptographic Erase. Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified in this guidance. Degaussing must not be performed as a sanitization technique on flash memory-based storage devices.
USB Removable Media *This includes Pen Drives, Thumb Drives, Flash Memory Drives, Memory Sticks, etc.*	
Clear:	Overwrite media by using organizationally approved and tested overwriting
	technologies/methods/tools. The Clear pattern should be at least two passes, to include a pattern in the first pass and its complement in the second pass. Additional passes may be used.
Purge:	Most USB removable media does not support sanitize commands, or if supported, the interfaces are not supported in a standardized way across these devices. Refer to the manufacturer for details about the availability and functionality of any available sanitization features and commands.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.

Notes:	For most cases where Purging is desired, USB removable media should be Destroyed.
Memory Cards *This includes SD, SDHC, MMC, Compact Flash Memory, Microdrive, MemoryStick, etc.*	
Clear:	Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear pattern should be at least two passes, to include a pattern in the first pass and its complement in the second pass. Additional passes may be used.
Purge:	N/A
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	None.
Embedded Flash Memory on Boards and Devices *This includes motherboards and peripheral cards such as network adapters or any other adapter containing non-volatile flash memory.*	
Clear:	If supported by the device, reset the state to original factory settings.
Purge:	N/A If the flash memory can be easily identified and removed from the board, the flash memory may be Destroyed independently from the disposal of the board that contained the flash memory. Otherwise, the whole board should be Destroyed.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	While Embedded flash memory has traditionally not been specifically addressed in media sanitization guidelines, the increasing complexity of systems and associated use of flash memory has complementarily increased the likelihood that sensitive data may be present. For example, remote management capabilities integrated into a modern motherboard may necessitate storing IP addresses, hostnames, usernames and passwords, certificates, or other data that may be considered sensitive. As a result, for Clearing, it may be necessary to interact with multiple interfaces to fully reset the device state. When this concept is applied to the example, this might include the BIOS/UEFI interface as well as the remote management interface. As with other types of media, the choice of sanitization technique is based on environmentspecific considerations. While the choice might be made to neither Clear nor Purge embedded flash memory, it is important to recognize and accept the potential risk and continue to reevaluate the risk as the environment changes.

Table A-9: RAM- and ROM-Based Storage Device Sanitization

RAM and ROM-Based Storage Devices	

Dynamic Random Access Memory (DRAM)	
Clear/ Purge:	Power off device containing DRAM, remove from the power source, and remove the battery (if battery backed). Alternatively, remove the DRAM from the device.
Destroy:	Shred, Disintegrate, or Pulverize.
Notes:	In either case, the DRAM must remain without power for a period of at least five minutes.
Electronically Alterable PROM (EAPROM)	
Clear/ Purge:	Perform a full chip Purge as per manufacturer's data sheets.
Destroy:	Shred, Disintegrate, or Pulverize.
Notes:	None.
Electronically Erasable PROM (EEPROM)	
Clear/ Purge:	Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	None.